21520641 Cao Thị Kim Cẩm

Bài 1. Chứng thực hàm băm

* Lưu đồ hoạt động của mô hình

Source A -> B

||

S

M



Compare

K

K

S

E{K, [M||E(PRa,H(M,S)]}

PUa

PRa

* Biểu thức minh hoạ mô hình: A -> B: E{K,[M||E(PRa, H(M,S)]}
* PRa là khoá bí mật của người gửi, S là khoá phiên, khoá K.
* Phân tích hoạt động:
* M (plaintext) sẽ được băm băm qua hàm băm (với chữ kí số), sau đó được mã hoá bởi khoá bí mật của người gửi, tạo **chữ ký số**. Mã hoá bởi khoá bí mật ở đây là để **chứng thực**.
* Chữ ký số này sẽ cùng với M sẽ được mã hoá bởi khoá K để **bảo mật**. Và được gửi đến người nhận (B).
* Người nhận khi đó sẽ giải mã thông điệp nhận được bằng khoá K, thu được plaintext M và chuỗi băm đã được mã hoá bởi khoá bí mật của người gửi.
* Người nhận tiếp tục giải mã chữ kí số để chứng thực thực thông tin người gửi, sẽ thu được chuỗi băm (M với hàm phi S).
* Người nhận đưa plaintext thu được qua hàm phi S và băm tạo chuỗi băm. Đem chuỗi băm này so sánh với chuỗi băm thu được để xác thực tính toàn vẹn.
* Ưu và nhược điểm của mô hình:
* Ưu điểm:

+ Đầy đủ các tính năng hơn: bảo mật, chứng thực, chữ kí số, tính toàn vẹn.

* Nhược điểm:

+ Mất thời gian hơn các mô hình cơ bản.

Bài 2: Chứng thực thông điệp và chữ ký số

Ảnh có chứa ảnh chụp màn hình, biểu đồ, Kế hoạch

Mô tả được tạo tự động

1. Open document → Document: Mở tài liệu.
2. Select hash function → Hash function: Lựa chọn hàm băm (ví dụ MD5, SHA1, SHA3,…)
3. Generate key → RSA key: tạo khoá RSA
4. RSA key ⇿ Provide certificate: chứng chỉ được cấp từ khoá RSA vừa tạo.
5. Provide certificate → Certificate: Cấp chứng chỉ
6. (7) Compute hash value : Tiến hành băm tài liệu.

(10) Thu được chuỗi băm.

(8) (11) RSA key → Encrypt hash value: Mã hoá chuỗi băm vừa thu được sau khi băm ở bước (10) bởi khoá RSA vừa tạo.

(9) Generate signature: Từ chứng chỉ được cấp, tạo chữ kí.

(12) Thu được chữ kí số (hàm băm được mã hoá).

(13)+(14) Gộp signature vào thông điệp ban đầu. Thu được thông điệp đã được ký.

(15) Sau khi mở tệp tài liệu, nếu thực hiện Cancel, sẽ tiến hành lưu trữ.

(16) Nếu thực hiện cả quá trình, sau khi hoàn tất sẽ tiến hành lưu trữ.

Bài 3: Giao thức bảo mật mạng (tên gọi, tầng hoạt động, đặc điểm, công dụng, thành phần chính)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Tên gọi | Tầng hoạt động | Đặc điểm | Công dụng | Thành phần chính |
| IPsec | Tầng mạng | Giao thức bảo mật chính tại lớp mạng.  Gồm giao thức chứng thực, mã hoá, trao đổi khoá. | Mã hoá quá trình truyền thông tin.  Đảm bảo tính toàn vẹn.  Xác thực giữa các giao tiếp.  Chống relay. | Thuật toán HMAC-SHA1, TripleDES-CBC và AES-CBC.  Transport và Tunel mode. |
| SSL/LTS | Tầng vận chuyển | Được dùng chủ yếu trong thực tế. | Bảo vệ những ứng dụng WWW và các giao dịch điện tử. | Record protocol và giao thức tầng ứn dụng (HTTP) |
| PGP và S/MIME | Tầng ứng dụng | Cơ chế bảo mật email.  Là một tiêu chuẩn Internet về định dạnh cho mail  Làm việc với khoá công khai để tìm kiếm khoá của người nhận. | Chứng thực thông điệp, mã hoá.  Định dạng tổng quát như chứng thực, nén ZIP,… |  |
| Kerberos | Tầng ứng dụng | Xác thực mạng máy tính hoạt động trên đường truyền không an toàn. | Chống việc nghe lén hay gửi lại gói tin cũ và đảm bảo tính toàn vẹn của dữ liệu. |  |
| SSH | Tầng ứng dụng | Tạo ra kết nối bảo mật giữa hai máy tính. | Mã hoá, chứng thực, định danh. |  |